REMARKS

The assignee of this application ("Applicant") respectfully requests reconsideration and allowance of the pending Application. After entry of this amendment, claims 1 - 22 will be pending, with claim 1 amended and claims 12 - 22 newly added for examination.

The pending Action rejected claims 1-11 under the judicially created doctrine of double patenting based on U.S. Patent No. 6,035,041 ("the '041 patent"). The pending Action contends that it would have been obvious to generate random values from shared values to increase the difficulty of an intruder "guessing the new keys." Applicant respectfully requests reconsideration of this rejection.

One example of shared randomness disclosed in the pending Application can be found on pages 9-10. Certain values, such as $\sigma_{i,j}$, are shared among entities participating in a distributed RSA signature system and are used to generate random values using a pseudo-random function, PRF. The random values in turn are used in computing partial results from which a final signature can be computed. Shares of the RSA secret key are also used in the computation of a partial result. The shared values are distinct from the RSA signature key and from shares of the RSA signature key.[1]

Nothing in the '041 patent suggests either a need for further protection against an intruder guessing new keys or a weakness for which a defense would be the use of shared randomness as disclosed in the pending Application. The '041 patent discloses, among other things, a proactive, optimal resilience,,public key cryptographic system that already employs daunting mechanisms

[1] The term "key" as used in the specification of the pending Application to refer to shared values for use in generating random numbers should not be read to imply that they are the same as, or derived from, signature keys. A convenient method for generating such shared values is a technique commonly known as "Diffie Hellman Key Exchange," however, such technique is not limiting.

to prevent intruders from guessing keys. In the examples of the '041 patent, a "key" is used in routine signing operations only in a distributed form as shares. A threshold number of authorized participants are required to invoke the use of a threshold number of shares to generate a digital signature. The system generates the digital signature without recombining the shares into "the" key. The key shares are changed periodically so that, even if an attacker were to obtain some (but less than a threshold number of) shares, such information would become useless over time. The administrators of the system may adjust the threshold number and the refresh period to provide an arbitrarily high degree of security (within the technical limits of computation power and communication capability) as might be desired for an application. Nothing in the '041 patent suggests a need for enhanced protection against an intruder guessing keys. Nothing identified in the pending Action identifies any other attack that could be ameliorated by use of shared randomness as disclosed in the pending Application, or any mechanism by which use of shared randomness would enhance security. As a countervailing consideration, it is widely understood in the art that addition of distributed processes imposes computational and communication burdens on the system, and unnecessary processes would not be added without a specific reason. With due respect, Applicant suggests that the reasoning of the pending Action, while well intentioned, is based on an incorrect premise.

The pending Action rejected claims 1 - 10 under 35 U.S.C. § 102 with a contention that those claims are anticipated by Gennaro *et al.* Applicant respectfully requests reconsideration of this rejection.

Claim 1, in its form *prior to* amendment, included steps of (a) computing shared values over a known context, and (b) generating random values using said shared values.[2] Gennaro *et al.* does not disclose such steps. Gennaro *et al.* discloses a distributed RSA system that uses shares of a secret RSA signature key. If, *arguendo*, the secret signature key is viewed as the claimed "shared value," it is not seen how Gennaro *et al.* discloses a step of generating random values using the shared values. Gennaro *et al.* discloses the calculation of a partial signature from a key share. That calculation does not introduce randomness and is not a step of generating a random value.

With respect to rejections of claims 2-10 as anticipated by Gennaro *et al.*, Applicant respectfully contends these claims will be seen as not anticipated once it is recognized that the claimed step of generating random values from shared values does not read on any values disclosed in Gennaro *et al.*

The pending Action rejected claims 1-4 and 9-11 under 35 USC § 102(e) over Brickell USP 5,867,578 ("Brickell"). With due respect, Applicant requests reconsideration of this rejection.

As a preliminary matter, the pending Action cites passages from Brickell at columns 9 and 10 which discuss a *non*-distributed signing algorithm. Because there is only a single signing entity, there is no distributed system, and these passages do not support an anticipation rejection.

The embodiment described in columns 11-12 of Brickell performs a distributed signing method that is described as a variant on the so-called El Gamal signature method. Entities called

[2] These limitations remain unchanged. Amendments to other parts of claim 1 are made to remove an unnecessary limitation and to clarify others with respect to aspects unrelated to the rejections of the pending Action. For example, the term "between" has been removed so as not to imply a process having precisely two devices.

RCA members each hold a share, x_i, of a secret key, x. During computation of a signature, each RCA member selects a random value k_i, and computes a value, r_i from the value k_i. If, *arguendo* the secret key, x, is considered to be the claimed "shared value," the random values k_i are not generated using the shared keys.

With respect to other claims rejected over Brickell, Applicant respectfully contends these claims will be seen as not anticipated once it is recognized that the claimed step of generating random values from shared values does not read on any values disclosed in Brickell.

CONCLUSION

Applicant respectfully submits that all rejections of the pending Action should be withdrawn on reconsideration, and that this application is in condition for allowance. Applicant respectfully requests a Notice to that effect and passage of this application to issuance. If, however, the Examiner is not convinced that the pending Application is in condition for allowance, Applicant requests an opportunity for the undersigned attorney to conduct a personal interview to discuss any remaining questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Assistant Commissioner for Patents, Box M.Fee, Washington, D.C. 20231"
on April 2, 2001
Signature Katie S. Lee
Typed or printed name Katie S. Lee

Respectfully submitted,

Stuart T.F. Huang
Registration No. 34, 184
Steptoe & Johnson, LLP
1330 Connecticut Avenue, N.W.
Washington, DC 20036
Tel: (202) 429-8056; Fax: (202) 429-3902